

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.



UNITED STATES PATENT AND TRADEMARK OFFICE

205
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/833,922	04/12/2001	Gregory O'Shea	208797	3840
23460	7590	09/14/2004	EXAMINER	
LEYDIG VOIT & MAYER, LTD TWO PRUDENTIAL PLAZA, SUITE 4900 180 NORTH STETSON AVENUE CHICAGO, IL 60601-6780				PARTHASARATHY, PRAMILA
ART UNIT		PAPER NUMBER		
2136				

DATE MAILED: 09/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/833,922	Applicant(s) O'SHEA ET AL.
	Examiner Pramila Parthasarathy	Art Unit 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 14 April 2003.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-25 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-25 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 5/14/01 & 4/15/03.
4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
5) Notice of Informal Patent Application (PTO-152)
6) Other: ____.

DETAILED ACTION

1. This action is in response to the communication filed on 04/15/2003. Claims 1 – 25 were received for consideration. No preliminary amendments were filed. Claims 1 – 25 are currently being considered.

2. Two initialed and dated copies of Applicant's IDS form 1449 are attached to the Office action.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

3. Claims 1- 25 are rejected under 35 U.S.C. 102(e) as being anticipated by Diffie et al (U.S. Patent Number Re. 36,946).

Regarding Claim 1, Diffie teaches and describes a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising:

creating authentication information, the authentication information including content data, a public key of the first computing device, a network address of the first computing device, and a digital signature, the network address having a portion derived from the public key of the first computing device, the digital signature generated by signing with a private key of the first computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data; and making the authentication information available to the second computing device (Fig. 4a – 4c, 5a; and Column 1 line 49 – Column 2 line 20 and Column 7 lines 6 – 45).

Regarding Claim 12, Diffie teaches and describes a computer-readable medium containing instructions for performing a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising:

creating authentication information, the authentication information including content data, a public key of the first computing device, a network address of the first computing device, and a digital signature, the network address having a portion derived from the public key of the first computing device, the digital signature generated by signing with a private key of the first computing device corresponding to the public key,

the digital signature generated from data in the set: the content data, a hash value of data including the content data; and making the authentication information available to the second computing device (Fig. 4a – 4c, 5a; and Column 1 line 49 – Column 2 line 20 and Column 7 lines 6 – 45).

Regarding Claim 13, Diffie teaches and describes a computer-readable medium having stored thereon a data structure (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the data structure comprising:

content data; a public key of a computing device; a network address of the computing device, the network address having a portion derived from the public key of the computing device; and a digital signature, the digital signature generated by signing with a private key of the computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data (Fig. 4a – 4c, 5a; and Column 1 line 49 – Column 2 line 20 and Column 7 lines 6 – 45).

Regarding Claim 20, Diffie teaches and describes 20. A method for a second computing device to authenticate content data made available by a first computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising:

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first

computing device, a first network address of the first computing device, and a digital signature; deriving a portion of a second network address from the public key of the first computing device; validating the digital signature by using the public key of the first computing device; accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data (Fig. 4a – 4c, 5a, 5b; and

Column 1 line 49 – Column 2 line 20 and Column 7 line 46 – Column 8 line 58).

Regarding Claim 25, Diffie teaches and describes 25. A computer-readable medium containing instructions for performing a method for a second computing device to authenticate content data made available by a first computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising:
accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature; deriving a portion of a second network address from the public key of the first computing device; validating the digital signature by using the public key of the first computing device; accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the

content data a hash value of data including the content data (Fig. 4a – 4c, 5a, 5b; and Column 1 line 49 – Column 2 line 20 and Column 7 line 46 – Column 8 line 58).

Claim 2 is rejected as applied about in rejecting Claim 1. Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the authentication information is made available to the second computing device by sending a message incorporating the authentication information to the second computing device (Column 7 lines 38 – 45).

Claims 3 and 14 are rejected as applied about in rejecting Claims 1 and 13. Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the content data include data for updating a network communications parameter for the first computing device (Column 9 line 46 – Column 10 line 58).

Claim 7 is rejected as applied about in rejecting Claim 1. Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the public key and the private key together form an uncertified key pair (Column 5 line 51 – Column 6 line 7).

Claims 8 and 17 are rejected as applied about in rejecting Claims 1 and 13.

Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the network address of the first computing device includes a route prefix portion and a node-selectable portion, and the node-selectable portion includes a portion of a hash value of data including the public key of the first computing device (Column 7 lines 6 – 29).

Claims 10 and 19 are rejected as applied about in rejecting Claims 1 and 13.

Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the authentication information further includes data for preventing a replay attack (Column 8 lines 12 – 58).

Claims 4 and 15 are rejected as applied about in rejecting Claims 3 and 14.

Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the first computing device is a mobile device, and wherein the network communications parameter is a care-of address of the first computing device (Column 7 line 6 – 10).

Claims 9 and 18 are rejected as applied about in rejecting Claims 1 and 13.

Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the node-selectable portion includes a portion of a hash value of data including the public key of the first computing device and a modifier selected for preventing address conflicts (Column 7 lines 23 – 45).

Claim 11 is rejected as applied about in rejecting Claim 10. Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the data for preventing a replay attack are in the set: time stamp, data identifying the second computing device as an intended recipient of the authentication information (Column 7 lines 6 – 45 and Column 8 lines 49 – 58).

Claims 5 and 16 are rejected as applied about in rejecting Claim 4. Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the second computing device is a home agent for the first computing device, and wherein the network address of the first computing device is a home address of the first computing device (Column 7 lines 6 – 10).

Claim 6 is rejected as applied about in rejecting Claim 4. Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the second computing device is a correspondent of the first computing device, and wherein the network address of the first computing device is a home address of the first computing device (Column 7 lines 6 – 10).

Claim 21 is rejected as applied about in rejecting Claim 20. Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), further comprising:

determining whether to accept the content data based on a time stamp in the authentication information (Column 7 lines 6 – 10 and Column 8 lines 18 – 32).

Claim 22 is rejected as applied about in rejecting Claim 20. Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the content data include data for updating a communications parameter for the first computing device, the method further comprising:

updating a record of a communications parameter for the first computing device (Column 7 line 38 – Column 8 line 67).

Claim 24 is rejected as applied about in rejecting Claim 20. Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the authentication information further includes a modifier, and wherein deriving includes appending the modifier to the public key of the first computing device before deriving a portion of the second network address (Column 8 lines 7 – 68).

Claim 23 is rejected as applied about in rejecting Claim 22. Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the communications parameter is a care-of address of the first computing device, and wherein updating includes updating a routing table maintained by the second computing device (Column 8 lines 7 – 68).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Hayosh (U.S. Patent Number 6,600,823) Apparatus and Method for enhancing check security.

Atkinson (U.S. Patent Number 5,511,122) Intermediate Network Authentication

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks, Washington, D.C. 20231 **or**

faxed to: (703) 872-9306 for all formal communications.

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Fourth Floor (Receptionist).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 703-305-8912. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Pramila Parthasarathy
Patent Examiner
703-305-8912
September 8, 2004


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100